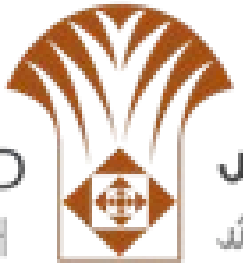


UNIVERSITE CADI AYYAD
MARRAKECH

جامعة القاضي عياض
مراكش

ENSA
Safi

Administration Réseaux Avancée sous GNU/Linux

Mohammed Madiafi
Département Informatique, Réseaux et Télécoms

Plan du cours

- Ch.0 : Introduction générale
- Ch.1 : Configuration du réseau local
- Ch.2 : Authentification des utilisateurs
- Ch.3 : Résolution des noms par DNS
- Ch.4 : Partage de fichiers et/ou d’imprimantes
- Ch.5 : Serveur Web
- Ch.6 : Serveur de bases de données
- Ch.7 : Serveur de messagerie
- Ch.8 : Sécurité des réseaux

Administrateur GNU/Linux

Administrateur :

super utilisateur

ayant les droit d'accès root

Administrateur GNU/Linux

- Il se charge de :
  - Configurer le système de base
  - Créer et gérer les comptes utilisateurs
  - Installer et configurer les logiciels
  - Installer et configurer les serveurs
  - Assurer la sécurité du système
  - Faire des sauvegardes
  - Surveiller le fonctionnement du système
  - Résoudre les problèmes

Administrateur GNU/Linux

- Connaissances requises :
  - Système d'exploitation,
  - Architecture des ordinateurs,
  - Réseaux,
  - Commandes et scripts Shell,
  - etc.

GNU/Linux

- GNU/Linux = GNU + Linux
- Un système d'exploitation libre
- 4 Droits de la licence GPL :
  - Partager
  - Étudier
  - Modifier
  - Destribuer

2 modes d'utilisation

- Mode Console (Mode commande)
  - Pour les utilisateurs expérimentés
  - Cas des serveurs
- Mode graphique
  - Pour les utilisateurs normaux
  - Gnome
  - Kde
  - Xwindows
  - etc.

Installation du système

- A l'aide
  - de CD/DVD/USB
  - du réseau
  - des sources
- Configuration matérielle requise
  - RAM
  - HDD
- Partitionnement

Systèmes de fichiers Linux

- /
- /etc
- /bin
- /sbin
- /root
- /home
- lost+found
- /var
- /boot
- /tmp
- /dev
- /usr
- /mnt
- /media

ORACLE
VM

VirtualBox

VirtualBox Graphical User Interface
Version 5.2.6 r120293 (Qt5.7.1)

Close

Intérêt de VirtualBox

Terminologie

- Hôte
  - Système physique
- Invitée
  - Système virtuel
- Machine virtuelle (MV)
  - Environnement créé par virtualbox pour exploiter le système virtuel

VBox : Configuration d'une MV

- Configuration réseau
  - NAT :
  - Accès par pont :
  - Réseau interne :
  - Réseau privé hôte :

Démonstration

- Installation de machines virtuelles
  - En utilisant un nouveau disque
  - En utilisant un disque existant
- Installation de plusieurs systèmes sur la même machine virtuelle
  - Utilisation de Gparted (installation à côté de Windows)
- Clonage / Export / Import

Gestion de systèmes de fichiers

- Créer/Modifier/Copier
  - GParted
  - fdisk
  - mkfs.*
  - mkisofs
  - dd
- Montage/Démontage
  - /dev/sdX
    - mount
    - umount
  - /etc/mtab
  - /etc/fstab
  - blkid (pour afficher UUID)

MBR vs GPT

	MBR (Master Boot Record)	GPT (GUID Partition Table)
Spécifications	aucune	UEFI
Nombre de partitions primaires autorisées	4	illimité (la configuration dépend du système d'exploitation ; pour Windows : 128)
Taille maximale de partition	2 téraoctets (2 000 gigaoctets)	18 exaoctets (18 milliards de gigaoctets)
Taille maximale du disque dur	2 téraoctets (2 000 gigaoctets)	18 exaoctets (18 milliards de gigaoctets)
Sécurité	secteurs de données sans total de contrôle	secteurs de données avec total de contrôle CRC32 et table de partitionnement GUID de sauvegarde
Nom de la partition	enregistré dans la partition	identifiant GUID unique + un nom comportant 36 caractères
Soutien aux configurations multiboot	faible	fort (grâce à l'installation du chargeur d'amorçage sur une partition séparée)

Tailles systèmes de fichiers

Nom du système de fichiers	Taille maximale d'un fichier	Taille maximale d'une partition	Journalisée ou non ?	Gestion des droits d'accès?
`Ext2` (Extended File System)	2 TiB	4 TiB	Non	Oui
`Ext3`	2 TiB	4 TiB	Oui	Oui
`Ext4`	16 TiB	1 EiB	Oui	Oui
`ReiserFS`	8 TiB	16 TiB	Oui	Oui
`BtrFS`	16 EiB	16 EiB	Oui	Oui
`Fat` (File Allocation Table)	2 GiB	2 GiB	Non	Non*
`Fat32`	4 GiB	8 TiB	Non	Non*
`Ntfs` \\(New Technology File System)	16 TiB	256 TiB	Oui	Oui*

Gestion de paquets

- Sous Debian
  - dpkg
  - apt
  - /etc/apt/sources.list
- Sous RedHat
  - rpm
  - yum (peut être installé sur Debian aussi)
  - /etc/yum.conf

Nom de la machine

- À l'aide d'une commande :
  - Hostname // Afficher le nom de la machine
  - hostname *MACHINE* // Editer le nom de la machine
- À travers un fichier de configuration
  - /etc/hostname

Noms des interfaces réseaux

- Numéros d'index fournis par Firmware/BIOS au péripherique branché (**eno1**)
- Numéros d'index fournis par Firmware/BIOS au slot PCI (**ens1**)
- Emplacement physique/géographique du connecteur du matériel (**enp2s0**)
- Adresse MAC de l'interface (**enx78e7d1ea46da**)
- Nommage classique (**eth0**, **wlan1**)

Interfaces réseaux
Noms prévisibles

- Noms stables à travers les redémarrages
- Noms stables même lorsque du matériel est ajouté ou retiré
- Noms stables lorsque les noyaux ou les pilotes sont mis à jour / modifiés
- Noms automatiquement déterminés sans configuration utilisateur
- Noms entièrement prévisibles (lspci)
- Sur toutes les distributions adoptant systemd

Interfaces réseaux
Noms prévisibles

- lspci
- /sys/devices/pci0000:00/0000:00:1c.3/0000:07:00.0/net/enp7s0
- ls /sys/class/net
- udevadm info –path=/sys/class/net/enp7s0f1

  (**en** dans "enp7s0f1" veut dire "**E**ther**N**et")
- udevadm info –path=/sys/class/net/wlp6s0

  (**wl** dans "wlp6s0" veut dire "**W**ire**L**ess")
- PCI geographical location : [P<domain> (if not 0)]p<bus>s<slot> [f<function>][d<dev_port>]

Interfaces réseaux
Infos sur les interfaces

- nmcli device show
-

Configuration d'une interface réseau à l'aide de « ifconfig » (net-tools)

- #afficher l'état des interfaces actuellement actives
  - ifconfig
- #afficher l'état de toutes les interfaces (actives ou inactives)
  - ifconfig -a
- #configurer une interface
  - ifconfig enp6s0 192.168.9.100
  - ifconfig enp6s0 netmask 255.255.255.0

Configuration d'une interface réseau à l'aide de « ifconfig » (net-tools)

- #ajouter une adresse à une interface
  - ifconfig enp0s3:enp0s31 192.168.9.200
- #enlever l'adresse ajoutée à une interface
  - Ifconfig enp0s3:enp0s31 down
- #Démarrer une interface
  - ifup enp0s3
- #Arrêter une interface
  - ifdown enp0s3
- #configuration à l'aide d'un serveur DHCP
  - dhclient enp0s3

Configuration d'une interface réseau
Interface Wi-Fi

- #affichage des infos sur les interfaces
  - iwconfig
- #lister les réseaux WIFI détectés
  - iwlist scanning
  - iwlist wlan0 scanning
- #connexion à un réseau WIFI ouvert
  - iwconfig wlan0 essid *WIFI781*

Configuration d'une interface réseau
Interface Wi-Fi

- sudo apt install wpasupplicant
- wpa_passphrase "ESSID" "passphrase" > /etc/wpa_supplicant.conf
- sudo wpa_supplicant -c /etc/wpa_supplicant.conf -i wlp3s0
- sudo wpa_supplicant -B -c /etc/wpa_supplicant.conf -i wlp3s0
- sudo dhclient wlp3s0

Table de routage

- #affichage de la table de routage du noyau
  - route
- #passerelle
  - route add -net 192.168.9.0 netmask 255.255.255.0 gw 192.168.9.7 dev enp0s3
  - route del -net 192.168.9.0 netmask 255.255.255.0 gw 192.168.9.7 dev enp0s3

Table de routage

- route del -net 192.168.9.0 netmask 255.255.255.0 gw 0.0.0.0 dev enp0s3
- route add default gw 192.168.9.1
- route add default gw 192.168.9.2 dev enp0s3
- route del default gw 192.168.9.1
- route del default gw 192.168.9.2 dev enp0s3
- route del default

Configuration d'une interface réseau à l'aide de « ip » (iproute2)

- #Afficher les info sur les interfaces réseaux
  - ip addr show (ou ip a)
  - ip addr show enp0s3
  - ip -4 -o addr show
  - ip -6 -o addr show
- #Ajouter une adresse à une interface
  - ip addr add 192.168.1.10/24 dev enp0s3
- #Supprimer l'adresse d'une interface
  - ip addr del 192.168.1.5/24 dev enp0s3

Configuration d'une interface réseau à l'aide de « ip » (iproute2)

- #Activer une interface
  - ip link set enp0s3 up
- #Désactiver une interface
  - ip link set enp0s3 down
- #Afficher la table de routage
  - ip route show (ou ip r)
- #Ajouter une passerelle par défaut
  - ip route add default via 192.168.1.1

Configuration d'une interface réseau à l'aide de « ip » (iproute2)

- #Afficher la table de routage
  - ip route show
- #Ajouter une passerelle
  - ip route add 10.10.20.0/24 via 192.168.50.10 dev enp3s0
- #Ajouter une passerelle par défaut
  - ip route add default via 192.168.50.10
- #Supprimer une passerelle
  - ip route del 10.10.20.0/24

Configuration permanente

- auto enp0s3
- allow-hotplug enp0s8
- iface enp0s3 inet dhcp
- iface enp0s3 inet6 dhcpv6
- iface enp0s8 inet static
- address 192.168.1.2/24
- gateway 192.168.1.1
- iface enp0s8 inet6 static
- address fec0:0:0:1::2/64
- gateway fec0:0:0:1::1

Configuration d'une interface réseau dans un fichier de configuration

Sous DEBIAN :

nano /etc/network/interfaces

- #Adresse Statique

```
iface enp0s3 inet static
    address 192.168.9.9
    netmask 255.255.255.0
    network 192.168.9.0
    broadcast 192.168.9.255
    gateway 192.168.9.1
    dns-nameservers 192.168.9.4
```

Configuration d'une interface réseau dans un fichier de configuration

Sous DEBIAN :

- #configuration à l'aide d'un serveur DHCP

  iface enp0s3 inet dhcp

Configuration d'une interface réseau dans un fichier de configuration

Sous REDHAT :

nano /etc/sysconfig/network-scripts/ifcfg-enp0s3

- #Adresse Statique

  DEVICE=enp0s3

  BOOTPROTO=none

  ONBOOT=yes

  IPADDR=192.168.9.100

  NETMASK=255.255.255.0

  GATEWAY=192.168.9.1

Configuration d'une interface réseau dans un fichier de configuration

Sous REDHAT :

- #configuration à l'aide d'un serveur DHCP

  DEVICE=enp0s3

  BOOTPROTO=dhcp

  ONBOOT=yes

Configuration d'une table de routage dans un fichier de configuration

Sous DEBIAN :

- vi /etc/network/interfaces
  - up ip route add 10.10.20.0/24 via 192.168.50.10 dev enp0s3

Sous REDHAT :

- vi /etc/sysconfig/network-scripts/route-eth0
  - 10.10.20.0/24 via 192.168.50.100 dev enp0s3

TCP WRAPPER

/etc/hosts.allow & /etc/hosts.deny

- #seule l'adresse 192.168.9.11 peut se connecter au service ftp de la machine
  - ftp:192.168.9.11
- #toutes les adresses du réseau 192.168.9.0 peuvent acceder à ssh
  - sshd:192.168.9.0/255.255.255.0
- #toutes les adresses du réseau 192.168.9.0 peuvent acceder à tous les services
  - ALL:192.168.9.0/255.255.255.0

Diagnostic réseau

- #tester la connectivité à un système distant
  - ping -c 3 google.fr
- #tester la connectivité à un système distant en affichant tous les routeurs y menant
  - traceroute google.fr
- #lister les interfaces actives dans le réseau
  - nmap -sn 192.168.5.0/24

Diagnostic réseau

- #afficher les connexions établies avec le système local (connexions actives)
  - netstat -n
- #afficher les processus responsables des connexions réseau
  - netstat -p

Plan du chapitre2

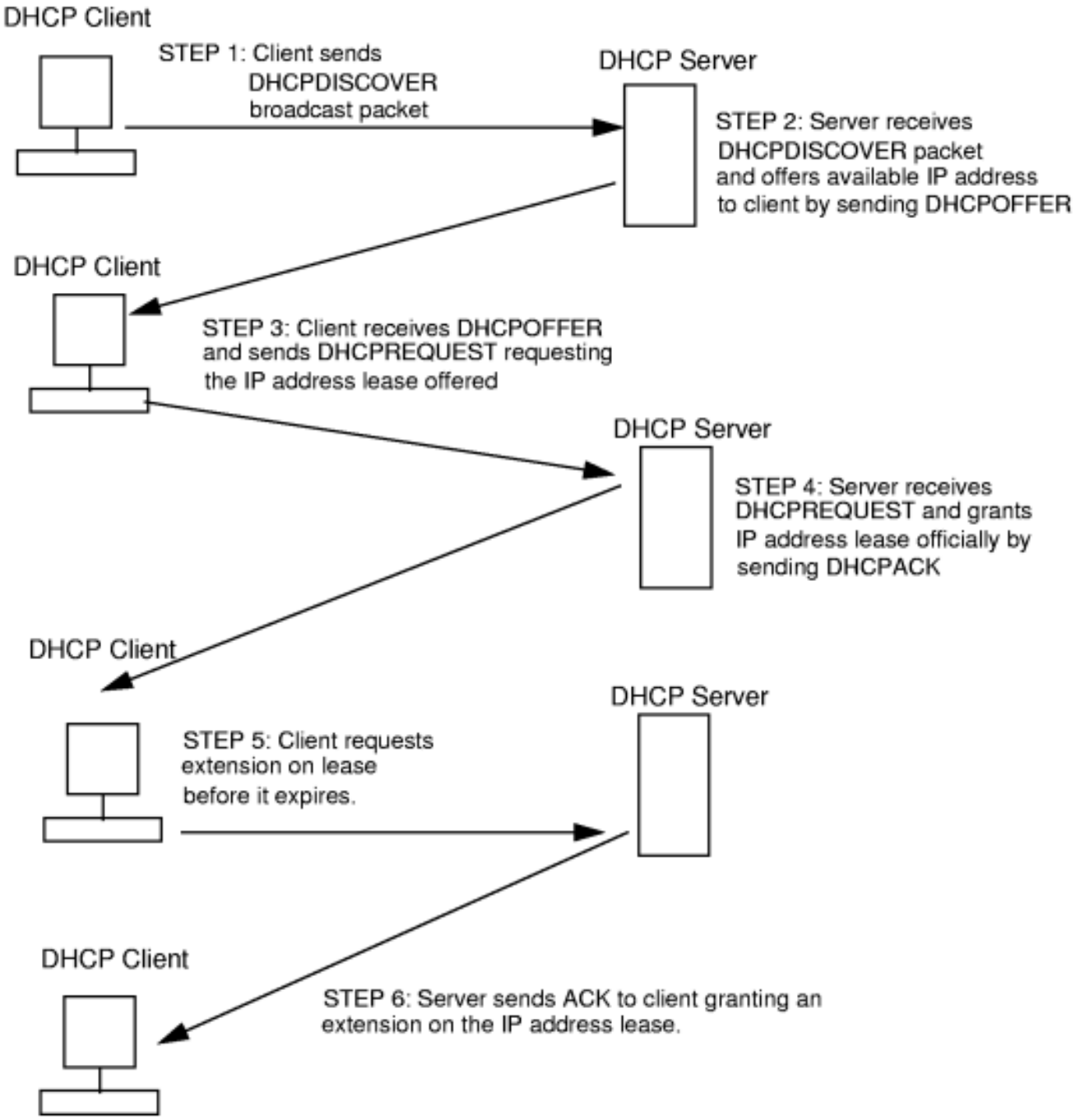
- Configuration automatique
  - DHCP
- Centralisation de fichiers de configuration
  - NIS
- Annuaire
  - LDAP

DHCP
(Dynamique Host Configuration Protocole)

DHCP
(Dynamique Host Configuration Protocole)

- Assigner à chaque machine du réseau
  - Une adresse IP unique,
  - Les adresses des serveurs DNS,
  - Les adresses des passerelles.
- Dispenser l'administrateur de la tâche difficile du suivi des adresses IP,
  - notamment lors de l'ajout d'une nouvelle machine.
- Éviter la duplication d'adresses IP.

Principe de fonctionnement



Installation

- Installation du serveur
  - isc-dhcp-server
- Installation du client
  - isc-dhcp-client

Configuration

- ATTENTION :
  - Tâchez à faire une sauvegarde de chaque fichier de configuration édité.

Configuration côté serveur

- /etc/dhcp/dhcpd.conf
  - Directives de fonctionnement
  - Options générales
  - Chaque ligne se termine par point-virgule.
- /etc/defaults/isc-dhcp-server
  - Modification du fichier de configuration
  - Choix d'interfaces d'écoute

Configuration côté serveur
/etc/dhcp/dhcpd.conf

- default-lease-time 600;
  - Duré par défaut en secondes attribuée à un client n'ayant pas spécifié une duré de bail.
- max-lease-time 7200;
  - Duré maximale de bail que peut demander un client.
- option domain-name-servers 192.168.9.4 ;
  - Adresses IP des serveurs de noms DNS.

Configuration côté serveur
/etc/dhcp/dhcpd.conf

#Configuration d'un segment basique

- subnet 192.168.9.0 netmask 255.255.255.0 {
  - range 192.168.9.100 192.168.9.200;
  - option routers 192.168.9.1;
- }

Configuration côté serveur
/etc/dhcp/dhcpd.conf

#Configuration avec plus d'options

- subnet 192.168.9.0 netmask 255.255.255.0 {
  - range 192.168.9.100 192.168.9.200;
  - option routers 192.168.9.1;
  - option domain-name-servers 192.168.9.3 , 192.168.9.4;
  - Default-lease-time 600 ;
  - max-lease-time 7200
- }

Configuration côté serveur
/etc/dhcp/dhcpd.conf

#Configuration spécifique d'une machine

- host machine {
  - hardware ethernet 08:00:27:6f:dd:60
  - Fixed-address 192.168.9.157 ;
  - option routers 192.168.9.1;
  - option domain-name-servers 192.168.9.3 ;
- }

Lancement du serveur

- /etc/init.d/isc-dhcp-server
  - status
  - start
  - stop
  - restart
  - force-reload

Configuration côté client

- /etc/network/interfaces
  - iface eth0 inet static

    address 192.168.9.9
    netmask 255.255.255.0
    network 192.168.9.0
    broadcast 192.168.9.255
    gateway 192.168.9.1
    dns-nameservers 192.168.9.4

  - iface eth0 inet dhcp

Demande d'une configuration automatique par un client

- Méthode1 :
  - dhclient eth0
- Méthode2 :
  - ifdown eth0
  - ifup eth0

Fichier de configuration client : /etc/dhclient.conf

Visualisation des baux DHCP
Côté serveur

- /var/lib/dhcp/dhcp.leases
  - Adresse louée
  - Adresse matérielle de l'interface concernée
  - Début et fin du bail

Visualisation des baux DHCP
Côté client

- /var/lib/dhcp/dhclient.leases
  - Serveur DHCP reconnu
  - Adresse louée
  - Masque du réseau
  - Adresse(s) serveur(s) DNS
  - Début et fin du bail
- /var/lib/dhcp/dhclient.eth0.leases
  - Spécifique à une interface (eth0 dans ce cas)

Visualisation des paquets échangés entre client et serveur DHCP

Tcpdump -i eth0 -n port 67 and port 68

- 01:25:06.163821 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:6f:dd:60, length 300
- 01:25:50.080980 IP 192.168.9.9.67 > 192.168.9.101.68: BOOTP/DHCP, Reply, length 300
- 01:25:50.093903 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:6f:dd:60, length 300
- 01:25:50.099202 IP 192.168.9.9.67 > 192.168.9.101.68: BOOTP/DHCP, Reply, length 300

Visualisation des paquets échangés entre client et serveur DHCP

Tcpdump -w cap -i eth0 -n port 67 and port 68

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transac
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transac
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transac
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transac
192.168.9.9	192.168.9.101	DHCP	342	DHCP Offer - Transac
192.168.9.9	192.168.9.101	DHCP	342	DHCP Offer - Transac
192.168.9.9	192.168.9.101	DHCP	342	DHCP Offer - Transac
192.168.9.9	192.168.9.101	DHCP	342	DHCP Offer - Transac
0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transac
192.168.9.9	192.168.9.101	DHCP	342	DHCP ACK - Transac
192.168.9.101	192.168.9.9	DHCP	342	DHCP Request - Transac

```
wire (2736 bits), 342 bytes captured (2736 bits)
musCo_6f:dd:60 (08:00:27:6f:dd:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
sion 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
., Src Port: bootpc (68), Dst Port: bootps (67)
```

Wireshark

```
08 00  27 6f dd 60 08 00 45 10   ........ 'o.`..E.
80 11  39 96 00 00 00 00 ff ff   .H...... 9.......
01 34  b7 8f 01 01 06 00 ca af   ...D.C.4 ........
00 00  00 00 00 00 00 00 00 00   ."...... ........
08 00  27 6f dd 60 00 00 00 00   ........ 'o.`....
```

Agent relai DHCP

- Envoyer des requêtes DHCP vers un serveur sur un réseau séparé.
- Pas de messages broadcast tramsmis par les routeurs :
  - Solution : Dhcrelay

Authentification des utilisateurs

NIS

- Objectif : Centralisation de l'administration de systèmes UNIX.
- /etc/passwd & /etc/shadow & /etc/hosts ...
- Appelé au départ « Yellow Pages ».
  - Le nom étant déjà enregistré pour une marque déposée, il a été remplacé par « Network information Service »
  - Les fichiers gardent tout de même l'abreviation « yp ».

NIS

- C'est un système client/serveur qui permet à un groupe de machines d'un domaine NIS de
  - partager un ensemble de fichiers de configuration communs.
- Ce qui permet à un administrateur système de
  - mettre en place des clients NIS avec un minimum de configuration
  - ajouter, modifier ou supprimer les informations de configuration à partir d'un unique emplacement.

Domaine NIS

- Un serveur maître NIS
  - Centralise les informations de configuration des machines (passwd, shadow, hosts, etc.)
- Un ou plusieurs serveurs esclaves NIS
  - Ils contiennent une copie de toutes les informations hébérgées par le serveur maître
- Les clients NIS
  - Ils envoient des requêtes vers un serveur NIS (pour l'authentification d'un utilisateur, pour la résolution du nom d'une machine, etc.)

Processus NIS

- rpcbind :
  - responsable de l'acitivation des RPC
    - Remote Procedure Call
    - ou appel de procédures distantes
  - doit tourner sur le sreveur et le client NIS.

Processus NIS

- ypbind :
  - Il récupère le nom de domaine NIS auprès du système, et en utilisant les RPC, il connecte le client au serveur NIS.
  - Si le processus ypbind meurt sur le client, aucune communication avec le serveur ne sera possible.
  - Après connexion au serveur, ypbind lui envoie de temps en temps des requêtes ping pour s'assurer qu'il marche encore.

Procesus NIS

- ypserv :
  - processus serveur proprement dit.
    - reçoit les requêtes des clients NIS
    - traduit le nom de domaine et le nom de table demandés en chemin d'accès à la base de données correspondante
    - transmet l'information de la base de données au client.

Procesus NIS

- ypserv :
  - doit tourner sur les serveurs NIS.
  - si le processus ypserv meurt, alors le serveur ne pourra plus répondre aux requêtes NIS
  - si dans ce cas, un serveur esclave est présent, il prendra la relève.

Processus NIS

- rpc.yppasswdd :
  - doit tourner sur les serveurs maître NIS.
  - permet aux clients de modifier leurs mots de passe NIS.
  - si rpc.yppasswdd ne tourne pas, la modification d'un mot de passe doit passer par l'ouverture d'une session sur le serveur.

Principe de fonctionnement

- La copie de référence de toutes les informations NIS est stockée sur le serveur NIS maître.
- Les bases de données utilisées pour le stockage de ces informations sont appelées tables NIS ou cartes NIS (“NIS maps”).
  - Ces tables se trouvent sous /var/yp/[domaine]
  - où [domaine] est le nom du domaine NIS.

Initialisation des tables

- Initialiser les tables NIS par ypinit
- Pour générer les tables pour un maître NIS :
  - on passe l'option -m à ypinit.
  - /usr/lib/yp/ypinit -m (ajout des esclaves)
- Pour générer les tables pour un esclave NIS :
  - on passe l'option -s à ypinit.
  - /usr/lib/ypypinit -s ip_maître_NIS

Sécurité NIS

- Pour des raisons de sécurité il est recommandé:
  - d'ajouter l'adresse du serveur NIS dans le fichier « /etc/yp.conf »
  - d'utiliser le fichier « /var/yp/securenets » pour restreindre l'accès à un ensemble donné de machines.

Installation

- Côté serveur :
  - apt-get install nis
- Côté client :
  - apt-get install nis
- Lors de l'installation, on choisit le nom du domaine.

Configuration côté serveur

- Désignation de la machine comme serveur NIS :
  - nano /etc/default/nis
    - NISSERVER=true
- Démarrage du service :
  - /etc/init.d/nis start

Configuration côté serveur

- Initialisation des tables NIS
  - /usr/lib/yp/ypinit -m
    - Exécuté une fois pour créer les tables
- cd /var/yp ; make
  - Exécuté chaque fois qu'il y a changement au niveau des fichiers d'informations du serveur (passwd, group, shadow, hosts, etc.).

Configuration côté serveur

- nano /etc/ypserv.securenet
  - 255.255.255.0 192.168.9.0
    - Après chaque modification de ce fichier, on redémarre le service NIS.
- nano /var/yp/Makefile
  - NOPUSH=false
    - pour configurer un esclave

Configuration côté client

- Choix du serveur NIS :
  - nano /etc/yp.conf
    - ypserver 192.168.9.100
- Configuration du service NSS :
  - nano /etc/nsswitch.conf
    - ajout de nis partout
- Configuration supplémentaire
  - nano /etc/passwd
    - +:::::/home/users:

Configuration côté esclave

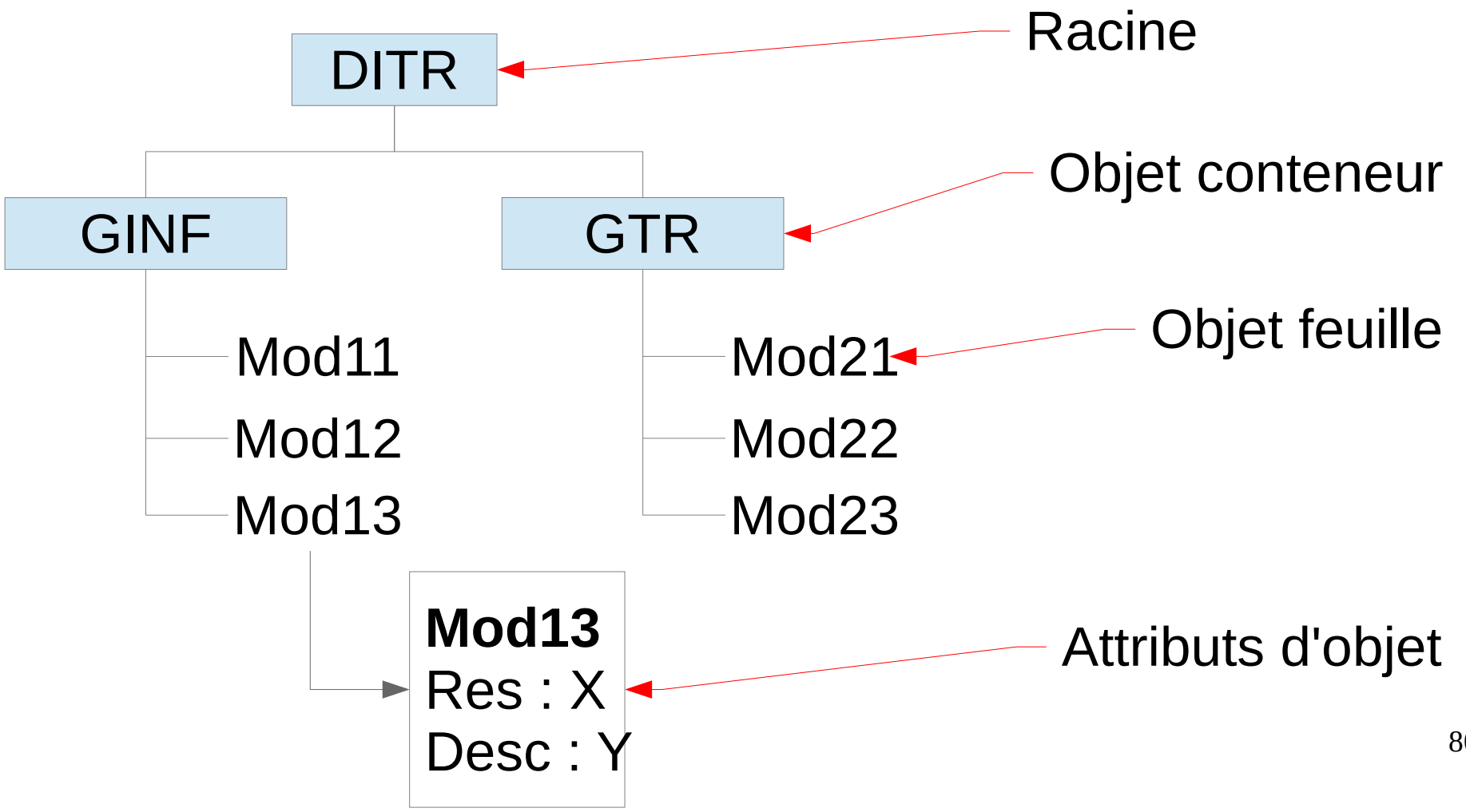
- Configiration client **+**
- Désignation de la machine comme esclave :
  - nano /etc/default/nis
    - NISSERVER=slave
- Import des tables depuis le serveur maître :
  - /usr/lib/yp/ypinit -s serveur_master

LDAP
(Light Directory Active Protocole)

- Un annuaire est un système de stockage d'informations qui se caractérise par :
  - Une consultation optimale
    - Mécanisme de recherche en fonction d'un critère donné.
  - Un modèle de stockage distribué
    - Possibilité de répartir les données sur plusieurs serveurs.
  - Une extensibilité des informations
    - Possibilité d'étendre la structure des données sans perte des entrées déjà définies.

Structure et terminologie

- Les données dans un annuaire LDAP sont organisées sous forme d'un arbre hiérarchique nommé DIT (Directory Information Tree).



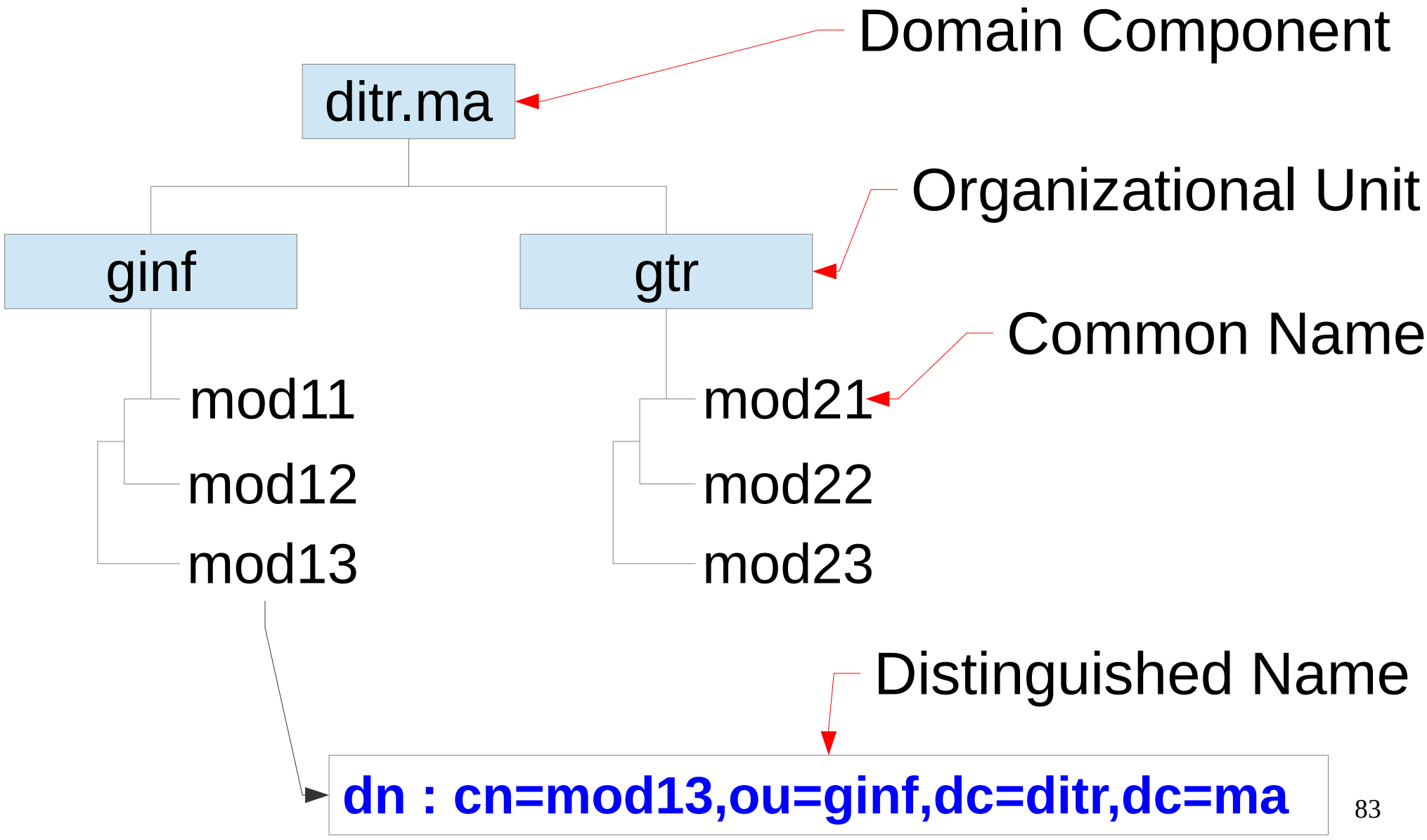
Schéma

- L'ensemble des types d'objets possibles dans un annuaires, et
- l'ensemble des attributs utilisables pour chaque objet.
- Le type de chaque objet est appelé « classe ».
- Une classe est définie par l'ensemble des attributs qui composent l'objet correspondant.

Désignation des objets

- Chaque entrée dans l'annuaire est désignée de deux façons :
  - Par son nom relatif RDN (Relative Distinguished Name) : ou=personne
  - Par son nom complet DN (Distinguished Name) : ou=personne,dc=societe,dc=com

Désignation des objets



Types courants des nœuds d'un DIT

dc (domain component)	Domaine
c (country)	pays
o (organization)	organisation
ou (organizational unit)	groupement
cn (common name)	nom

Format LDIF
(LDAP Interchange Format)

- Format de fichier définie par le protocole LDAP.
- Un fichier LDIF peut contenir :
  - Des descriptions d'entrées de l'annuaire ;
  - Des valeurs d'attributs pour les entrées de l'annuaires ;
  - Des instructions de traitements pour le serveur.

Ficher LDIF

- Exemple1 :
  - définition du groupement (ou unité organisationnelle) « ginf » du domaine « ditr.ma »

dn : ou=ginf,dc=ditr,dc=ma

objectClass : organizationalUnit

objectClass : top

ou : ginf

Ficher LDIF

- Exemple2 :
  - définition d'un « étudiant » du groupement « ginf » du domaine « ditr.ma »

dn : cn=etudiant1,ou=ginf,dc=ditr,dc=ma

objectClass : Person

objectClass : top

cn : etudiant1

sn : Foulane

telephoneNumber : +212 612 345 678

Connexion au serveur LDAP

- Session : un client doit créer une session avec un message « bind » et la fermer avec un message « unbind ».
- Pour établir la connexion, le client doit fournir l'adresse du serveur, le port utilisé et la version du protocole.
- Les comptes de connexion sont fournis sous la forme d'une entrée à laquelle est associé un mot de passe.
- Ex. d'entrée: cn=admin,dc=societe,dc=com

Interrogation d'un serveur LDAP

- Une requête LDAP a la forme :

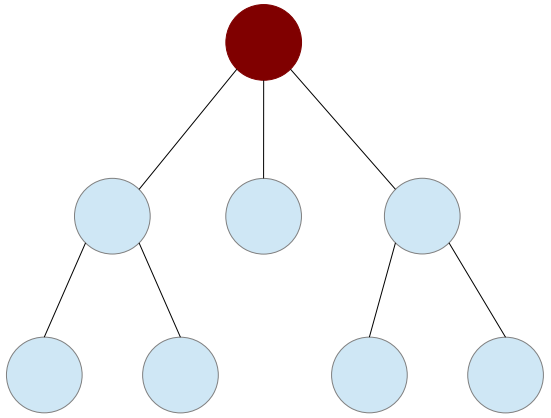
  Base ? Attributs ? Portée ? Filtre

  1. Base qui désigne le point d'entrée dans l'annuaire où commence la recherche.
  2. Attributs séparés par des virgules à fournir en réponse.
     - Si ce champs est vide ou s'il contient *, tous les attributs sont fournis.

Interrogation d'un serveur LDAP

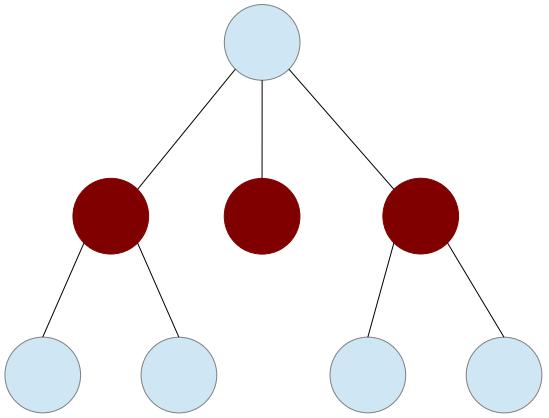
3. Portée ou scope qui spécifie l'emplacement dans l'arbre DIT des objets fournis en réponse. Il accèpte 3 valeurs : base, one et sub.

base



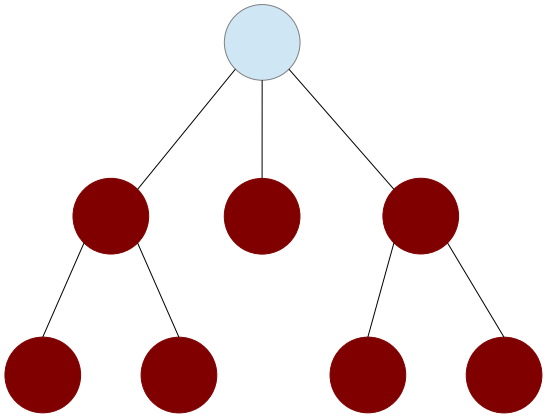
Seul l'objet de base est fourni

one



Les objets du 1èr niveau sont fournis

sub



Tous les objets du niveau inférieur sont fournis

Interrogation d'un serveur LDAP

4. Filtre qui spécifie les critères sur les attributs.
   - La forme est : (*attribut opérateur valeur*
   - (telephoneNumber=(212)*) fournira les objets dont l'attribut telephoneNumber commence par 212.
   - Les opérateurs possibles : **=** , **~=** , **<=** , **>=**
   - La combinaison de critères se fait à l'aide des opérateurs booléens : **|** , **&** , **!** :
     - (& (sn=Flane)(telephoneNumber=*1))

Opérations sur les entrées de l'annuaire

- Ajouter / supprimer une entrée
- Modifier une entrée
- Ajouter / supprimer un attribut
- Modifier la valeur d'un attribut

Ajouter une entrée (add)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : add

  objectClass : top

  objectClass : <*classe*>

  <*attribut*> *:* <*valeur*>

  <*attribut*> *:* <*valeur*>

Supprimer d'une entrée (delete)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : delete

Modifier une entrée (modify)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : modify

  add : <*attribut*>

  <*attribut*> *:* <*valeur1*>

  <*attribut*> *:* <*valeur2*>

Modifier une entrée (modify)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : modify

  delete : <*attribut*>

Modifier une entrée (modify)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : modify

  delete : <*attribut*>

  <*attribut*> *:* <*valeur1*>

  <*attribut*> *:* <*valeur2*>

Modifier une entrée (modify)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : modify

  replace : <*attribut*>

  <*attribut*> *:* <*valeur1*>

  <*attribut*> *:* <*valeur2*>

Modifier le nom relatif d'une entrée (modrdn)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : modrdn

  newrdn : *<nouveau nom relatif>*

  newSuperior : *<nouveau parent>*

  deleteOldrdn : *<1 ou 0>*

Modifier le nom absolu d'une entrée (moddn)

- Dans un fichier LDIF :

  dn : <*nom*>

  changeType : moddn

  newrdn : *<nouveau nom relatif>*

  newSuperior : *<nouveau parent>*

  deleteOldrdn : *<1 ou 0>*

Service LDAP

- Installation côté serveur
  - apt-get install slapd
  - apt-get install ldap-utils
- Installation côté client
  - apt-get install ldap-utils

Configuration côté serveur

- Configuration du service :
  - dpkg-reconfigure slapd
    - On choisit le nom du domaine, le mot de passe, version LDAP, etc.

Ajout d'une entrée

dn: uid=toto,dc=ensas,dc=ma

objectClass: posixAccount

objectClass: person

uid: toto

cn: toto

sn: toto

uidNumber: 2000

gidNumber: 2000

homeDirectory: /home/users

loginShell: /bin/bash

userPassword:{SSHA}nRkpzvpuhDhZ+OFVwu

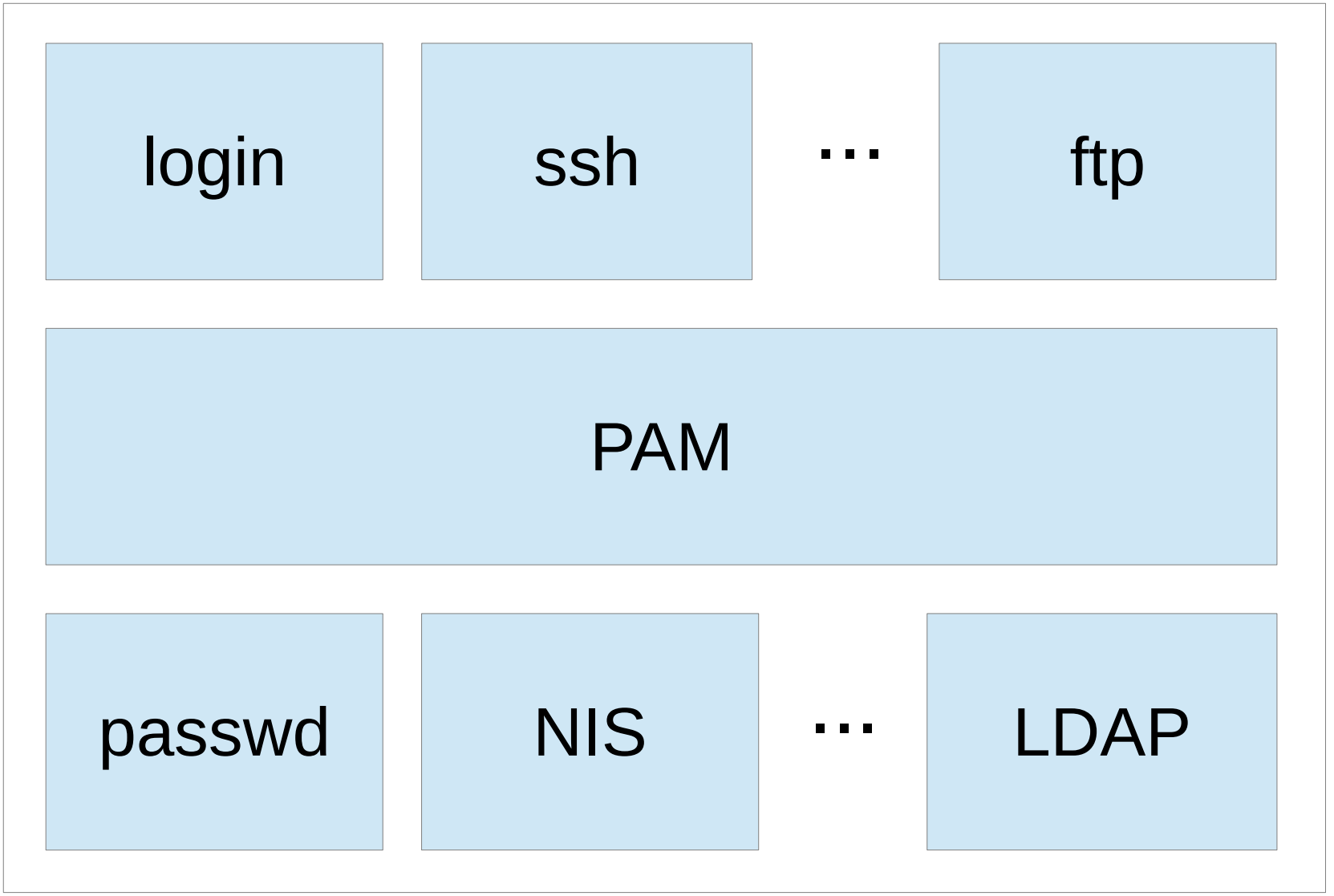
Ajout d'une entrée

- Ajout de l'entrée à l'aide de ldapadd :
  - ldapadd -x -D cn=admin,dc=ensas,dc=ma -W -f fichier.ldif
- Vérification à l'aide de ldapsearch:
  - ldapsearch -x -b uid=toto,dc=ensas,dc=ma

Configuration côté client

- Vérification depuis le client
  - ldapsearch -x -b -h 192.168.9.100 dc=ensas,dc=ma
- ou bien:
  - nano /etc/ldap/ldap.conf
    - host 192.168.9.100
    - base dc=ensas,dc=ma
  - ldapsearch -x

Authentification à l'aide de LDAP (PAM)



Fonctionnement du PAM

- Une application demande au PAM si un utilisateur peut se connecter.
- PAM appelle des modules fonctionnels pour exploiter une méthode d'authentification.
- Si le résultat est positif, l'utilisateur a fourni les bons éléments d'authentification ;
  - Dans ce cas, PAM renvoie l'autorisation de connexion à l'application.

Authentification à l'aide de LDAP

- apt-get install libnss-ldap libpam-ldap nscd
  - Une configuration est choisie lors de l'installation
- Modification de /etc/nsswitch.conf
- Vérification de :
  - /etc/pam.d/common-account
  - /etc/pam.d/common-auth
  - /etc/pam.d/common-session

Plan de la 3ème partie

- Résolution des noms par DNS
- Partage de fichiers avec NFS
- Partage de fichiers avec FTP
- Partage d'imprimantes avec CUPS
- Partage de données et de ressources avec SAMBA

DNS

- Avec les fichiers hosts, chaque machine dispose de sa propre base de données de noms.
- Sur des réseaux importants, cette base de données dupliquée n'est pas simple à maintenir.
- Avec un service de résolution de noms, la base de données est localisée sur un serveur.
- Un client qui désire adresser un hôte regarde dans son cache local, s'il en connaît l'adresse. S'il ne la connaît pas, il va interroger le serveur de noms.

DNS

- Avec un serveur DNS, un administrateur n'a plus qu'une seule base de données à maintenir. Il suffit qu'il indique sur chaque hôte, quelle est l'adresse de ce serveur.
- Deux cas sont possibles :
  - L'adresse du serveur DNS est renseignée de manière statique dans les fichiers de configuration.
  - L'adresse du serveur DNS est affectée par un serveur DHCP.

DNS
Domain Name Server

- Le service DNS = service de résolution de noms de domaine.
- Il permet d'adresser un hôte par un nom, plutôt que de l'adresser par une adresse IP.
- Structure d'un nom d'hôte :
  - NomHôte**.**NomDomaine
  - serveur**.**ensas.ma

Domaine

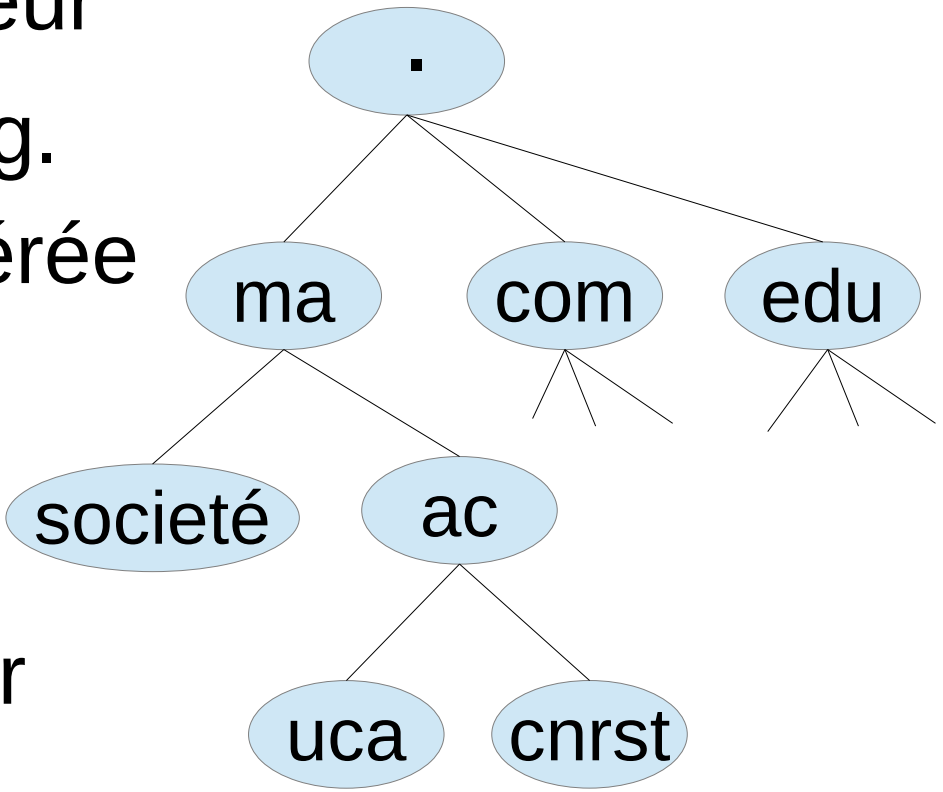
- Un domaine est un sous-arbre de l'espace de nommage.
  - Exemple : .com est un domaine, il contient toute la partie hiérarchique inférieure de l'arbre sous jacente au noeud .com.
- Un domaine peut être organisé en sous domaines.
  - Exemple : .google.com est un sous domaine du domaine .com.

Nom de domaine

- Le nom de domaine identifie une organisation dans l'internet
  - Exemple : google.fr, yahoo.com, etc.
- Chaque organisation dispose d'un ou plusieurs réseaux. Ces réseaux sont composés de noeuds (postes, serveurs, routeurs, imprimantes) pouvant être adressés.
  - Exemple : « ping serveur.ensas.ma » permet d'adresser la machine qui porte le nom d'hôte « serveur », dans le domaine (organisation) « ensas.ma ».

Zones DNS

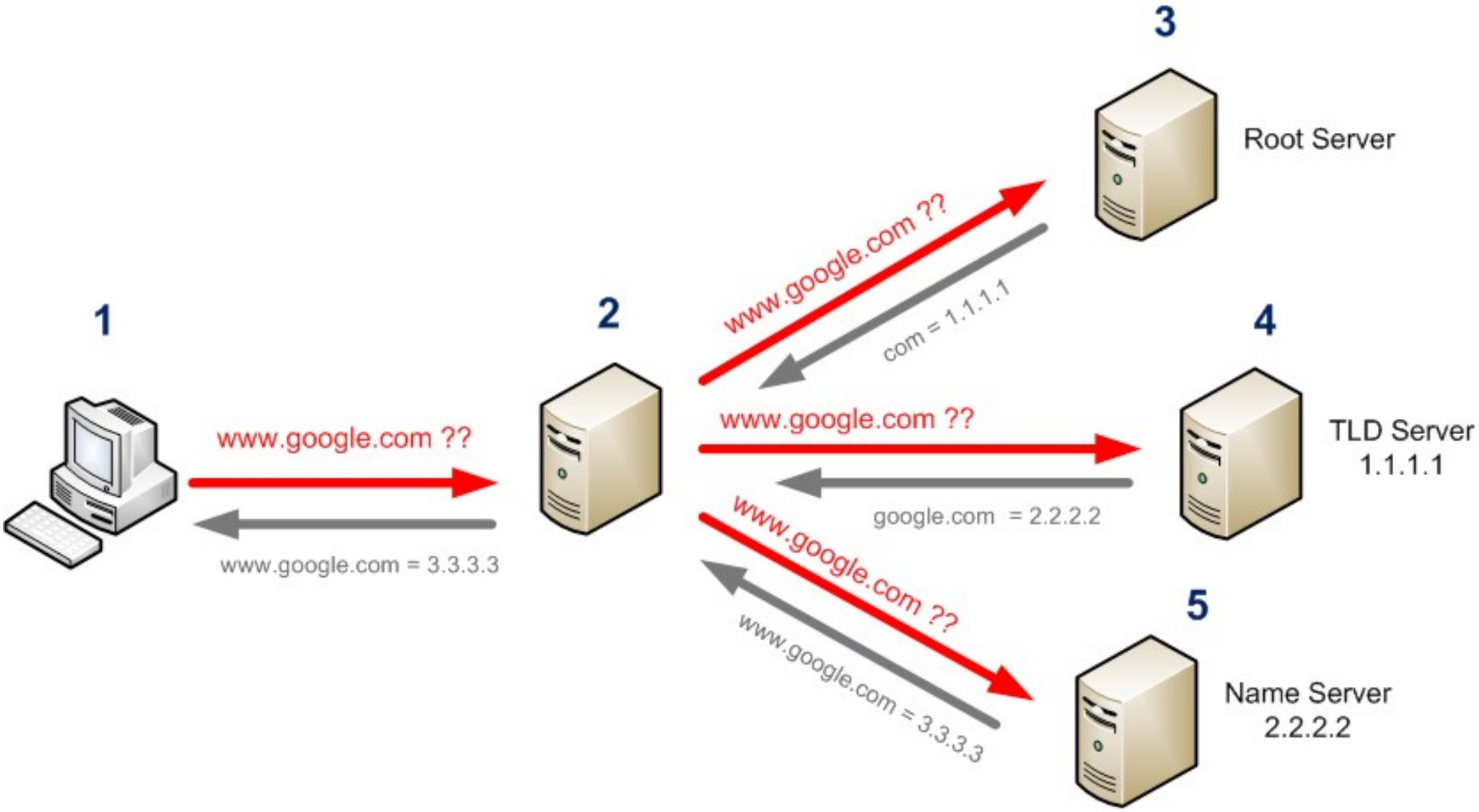
- Chaque niveau de l'arborescence DNS est une zone DNS.
- La zone « . » est la racine qui contient tous les niveaux de niveau supérieur
  - tels que com, ma, fr, org.
- Chaque zone peut être gérée par un serveur.
  - Le serveur hébérgeant les données de la zone « ac » est consulté pour résoudre tout nom se terminant par « ac.ma ».



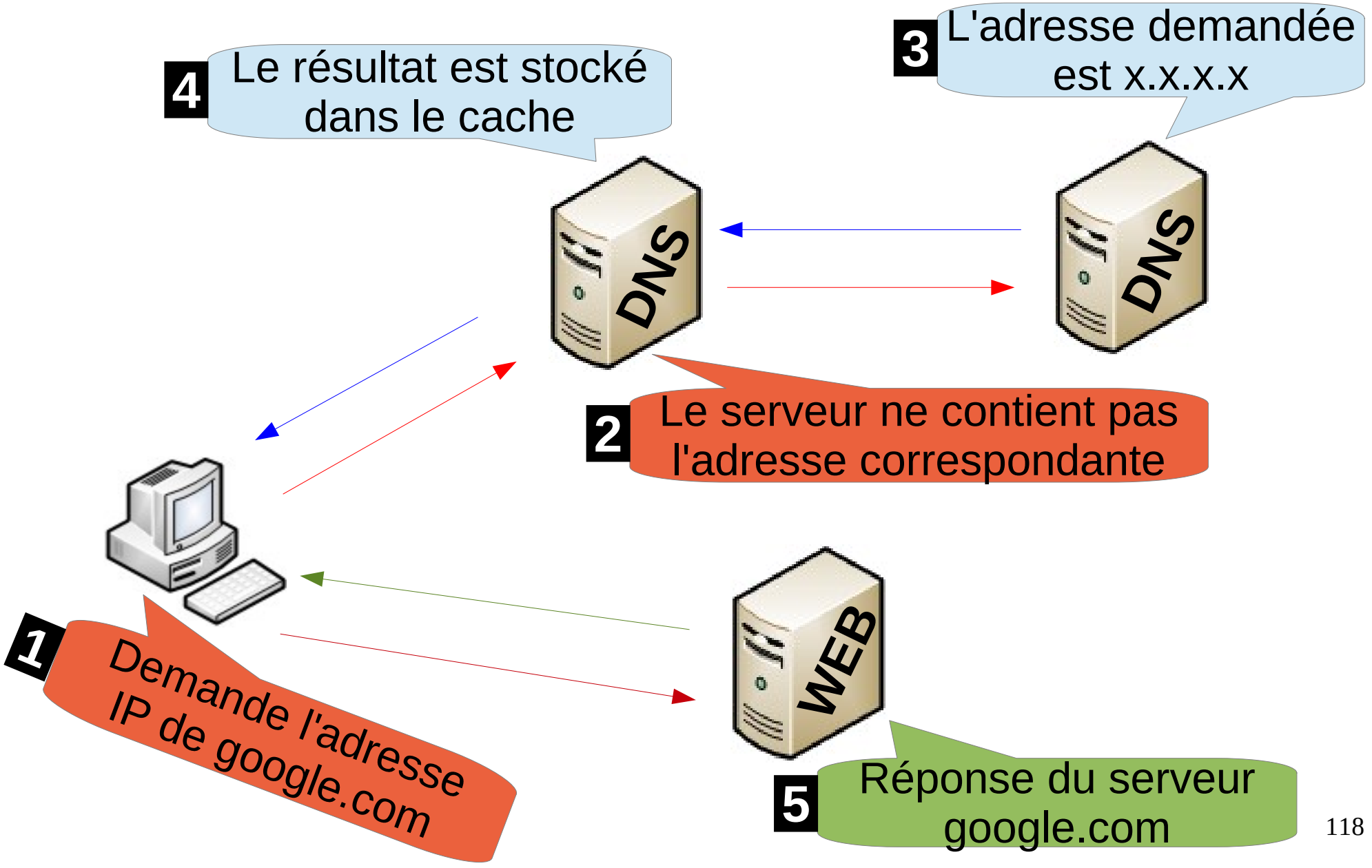
Mécanisme de résolution de noms

- Une application demandant une résolution de nom s'adresse au « resolver » du système d'exploitation.
- Le resolver envoie une requête à un serveur DNS local référencé dans un fichier de configuration.
- Si le serveur interrogé dispose de l'information demandée, il répond directement.

Mécanisme de résolution de noms



Mécanisme de résolution de noms



Enregistrements

- Les enregistrements sont des informations permettant de correspondre un nom à une adresse IP ou à une autre information.
- Dans les fichiers de configuration d'un serveur DNS, on utilise des noms de domaines pleinement qualifiés (FQDN : Fully Qualified Domain Name)
  - Exemple : « www.google.com. » : www est représenté par un enregistrement dans la zone google.com. La présence du point après com est obligatoire.

Enregistrement de type A

- L'enregistrement qui fait correspondre une adresse IP à un nom.
  - www.google.com est un enregistrement de A dans la zone google.com.
  - Il correspond au serveur Web hébérgeant la page d'accueil google.
- Syntaxe :
  - www IN A 196.12.217.53

Enregistrement de type AAAA

- Fait correspondre un nom à une adresse IPv6
- Syntaxe :
  - www IN AAAA
    2001:670 :12:234a:24:16bb:ab21:1234

Enregistrement de type PTR

- Un enregistrement PTR permet de faire l'inverse de A.
- C'est à dire la résolution inverse.
- Il existe dans des zones particulières nommées « in-addr.arpa »
- Syntaxe : Zone 168.192.in-addr.arpa
  - 9.10 IN PTR serveur1.domaine.fr

    (ça veut dire que l'adresse de serveur1.domaine.fr) est 192.168.9.10.

Enregistrement de type CNAME

- CNAME : Canonical Name
- Ceci permet de correspondre à un nom un autre nom ou alias.
- Syntaxe :
  - Serveur1 IN CNAME imprimantes

Enregistrement de type MX

- MX (MAIL EXCHANGE) : Indique le serveur de messagerie pour le domaine
- Ça permet de faire savoir à des agents de transfert de messagerie quel est le serveur destinataire final d'un courrier.
- Syntaxe : Zone domaine.fr
  - mail IN MX 192.168.9.100

    (un message envoyé à une adresse se terminant par @domaine.fr sera dirigé au serveur mail.domaine.fr)

Enregistrement de type SOA

- SOA (START OF AUTHORITY) : Détermine le serveur ayant la responsabilité de la zone.
- Toute zone fonctionnelle a un enregistrement SOA.
- Syntaxe :
  - Domaine.fr. IN SOA ns.hebergeur.fr

Enregistrement de type NS

- NS (NAME SERVER) : indique les serveurs de noms pour la zone.
- Toute zone fonctionnelle a au moins un enregistrement NS.
- Syntaxe :
  - Domaine.fr. IN NS ns.hebergeur.fr

BIND
Berkeley Internet Name Domain

- Le paquet logiciel « bind » comporte le démon « named » qui répond aux requêtes DNS.
- Sur le client, il existe un ensemble de bibliothèques permettant la résolution de nom en intérogeant un serveur DNS.
  - dig
  - nslookup
  - host

Installation

- Côté serveur :
  - apt-get install bind9
- Côté client :
  - apt-get install dnsutils

Configuration (côté serveur)

- /etc/bind/named.conf
  - Include "chemin_de_fichier_zone"
  - options { forwarders { A . B . C . D } }
  - allow-query { réseaux-autorisés }
  - zone "nom_de_zone1" {
    type master ;
    file "chemin_fichier_de_zone1" ;
    }

Configuration (côté serveur esclave)

- /etc/bind/named.conf
  - zone "nom_de_zone2" {

```
        type   slave ;
        masters  {   A.B.C.D   }
        file  "/var/fichier_de_zone2" ;
}
```

Exemple de zone directe

- $TTL 86400
- pas.net. IN SOA serv.pas.net root.pas.net. (
  2 ;serial
  604800 ;refresh
  86400 ;retry
  2419200 ;expire
  86400 ;negative)
- pas.net. IN NS serv.pas.net.
- serv.pas.net. IN A 192.168.9.100
- web IN CNAME serv.pas.net.

Exemple de zone directe

- Numéro de série (serial) : Identifie la version de la zone ; quand on modifie le fichier de zone, on incrémente ce numéro. Le format conseillé est le suivant : YYYYMMDDxx.
- Rafraîchissement (refresh) : intervalle en secondes destiné au serveur secondaire pour rafraîchir son fichier de zone (nombre décimal entier sur 8 chiffres). Cette valeur peut être élevée si on a maintenu l'option "notify yes" au niveau du serveur maître.

Exemple de zone directe

- Tentatives (retry) : intervalle en secondes avant de recontacter le serveur principal en cas d'échec de la demande de rafraîchissement.
- Expiration (expire) : indique le temps en secondes, au bout duquel un serveur secondaire doit éliminer toutes les informations de zone s'il n'a pas pu contacter le serveur (cette valeur doit être élevée).

Exemple de zone inverse

- $TTL 86400
- 168.192.in-addr.arpa. IN SOA serv.pas.net. root.pas.net. (

  2 ;serial

  604800 ;refresh

  86400 ;retry

  2419200 ;expire

  86400 ;negative)
- 168.192.in-addr.arpa. IN NS serv.pas.net.
- 100.9 IN PTR serv.pas.net.

Configuration (côté client)

- /etc/resolv.conf
  - Nameserver 1.1.1.1
  - Nameserver 2.2.2.2
  - Nameserver 3.3.3.3

Partage de données et de ressources

NFS

- NFS : Network File System
- Protocole historique de partage de fichiers sur les systèmes Linux/Unix.
- Avantages :
  - Rapidité.
  - Simplicité de mise en œuvre.

Installation

- Côté serveur :
  - apt-get install nfs-kernel-server
- Côté client :
  - apt-get install nfs-common

Partages à l'aide de NFS

- Les partages sont
  - déclarés pour un répertoire local
  - accessibles à certains clients avec certaines options
- Pour déclarer un partage ponctuel :
  - exportfs adresse_client : /chemin_du_partage
- Pour déclarer un partage permanent :
  - /etc/exports : chemin_partage   adresse_client
- Pour afficher les partages actifs :
  - La commande « exportfs »

Options de partage

ro	Accès en lecture seule
rw	Accès en lecture et écriture
sync	Accès en écriture synchrone. Les modifications sont écrites immédiatement.
async	Accès en écriture asynchrone. Utilisation d'un cache en écriture.
root_squash	Le compte root perd ses prérogatives sur le partage.
no_root_squash	Root conserve ses prérogatives sur le partage.

Partage de données à l'aide de FTP

- FTP : File Transfer Protocol
- L'un des premiers protocoles permettant le partage entre deux ordinateurs.
- Employé avant la création du protocole SMTP pour transférer les messages électroniques d'un ordinateur à un autre.
- Utilisé actuellement par les hébérgeurs de sites web pour permettre aux clients de mettre à jours leurs données.

Installation

- Côté serveur
  - apt-get install pure-ftpd
- Côté client
  - apt-get install ftp

Ajout d'un partage
(Première méthode)

- Création d'un utilisateur ayant comme répertoire personnel le dossier à partager(côté serveur)
  - adduser ftpuser --home /var
- Test (côté client)
  - ftp adresse_serveur_FTP

Ajout d'un partage
(Deuxième méthode)

- Ajout d'un compte virtuel (côté serveur)
  - pure-pw useradd ftpuser -u unixuser -d /var/partage
  - pure-pw usermod ftpuser -N 10
  - pure-pw mkdb
  - ln -s /etc/pure-ftpd/conf/PureDB /etc/pure-ftpd/auth/50pure
  - /etc/init.d/pure-ftpd restart
- Test (côté client)
  - ftp adresse_serveur_FTP

Partage d'imprimantes par CUPS

- CUPS : Common Unix Printing System
- Système d'impression sous Linux/Unix
- Prend en charger le protocole d'impression internet (IPP : Internet Printing Protocol)

Partage d'imprimantes par CUPS

- Côté serveur :
  - apt-get install cups
- Côté client :
  - apt-get install cups-client

Gestion d'imprimantes

- Ajout d'une imprimante :
  - lpadmin -p imprimante -v URI -m PPD -E
  - Imprimante : nom quelconque
  - URI : port ou méthode de connexion (lpinfo -v)
  - PPD : Description de l'imprimante (lpinfo -m)
- Imprimante par défaut :
  - lpadmin -d imprimante
- Test :
  - lp fichier_à_imprimer -d imprimante
  - lp fichier_à_imprimer

Configuration

- Côté serveur :
  - /etc/cups/cupsd.conf
    - Listen IP_serveur : 631
    - Allow adr_réseau / masque_réseau
  - /etc/cups/printers.conf
    - Shared Yes
- Côté client :
  - /etc/cups/client.conf
    - ServerName adr_serveur

cups-pdf

- Imprimante virtuelle pour le test
- Ou créateur de fichiers PDF
- Installation
  - apt-get install cups-pdf
- Impression
  - lp fichier.txt
  - Le PDF résultant est stocké dans /home/user/PDF ou /var/spool/cups-pdf
  - Pour le changer : /etc/cups/cups-pdf.conf

Partages à l'aide de SAMBA
Installation

- Côté serveur :
  - apt-get install samba
- Côté client :
  - apt-get install smbclient
  - apt-get install cifs-utils

Configuration
(Côté serveur)

- /etc/samba/smb.conf
  - ....
  - [partage]

    comment = dossier partagé

    browseable = yes

    read only = no

    path = /chemin_du_partage
- Création d'un mot de passe SMB
  - smbpasswd -a user

Côté client
Connexion à l'aide de smbclient

- Smbclient //adr_serveur/partage -U user
- On aura une interface qui ressemble à celle de FTP
- Se déplacer dans l'arborescence : cd
- Envoyer des fichiers vers le partage : put
- Récupérer des fichiers : get

Côté client
Montage permanent

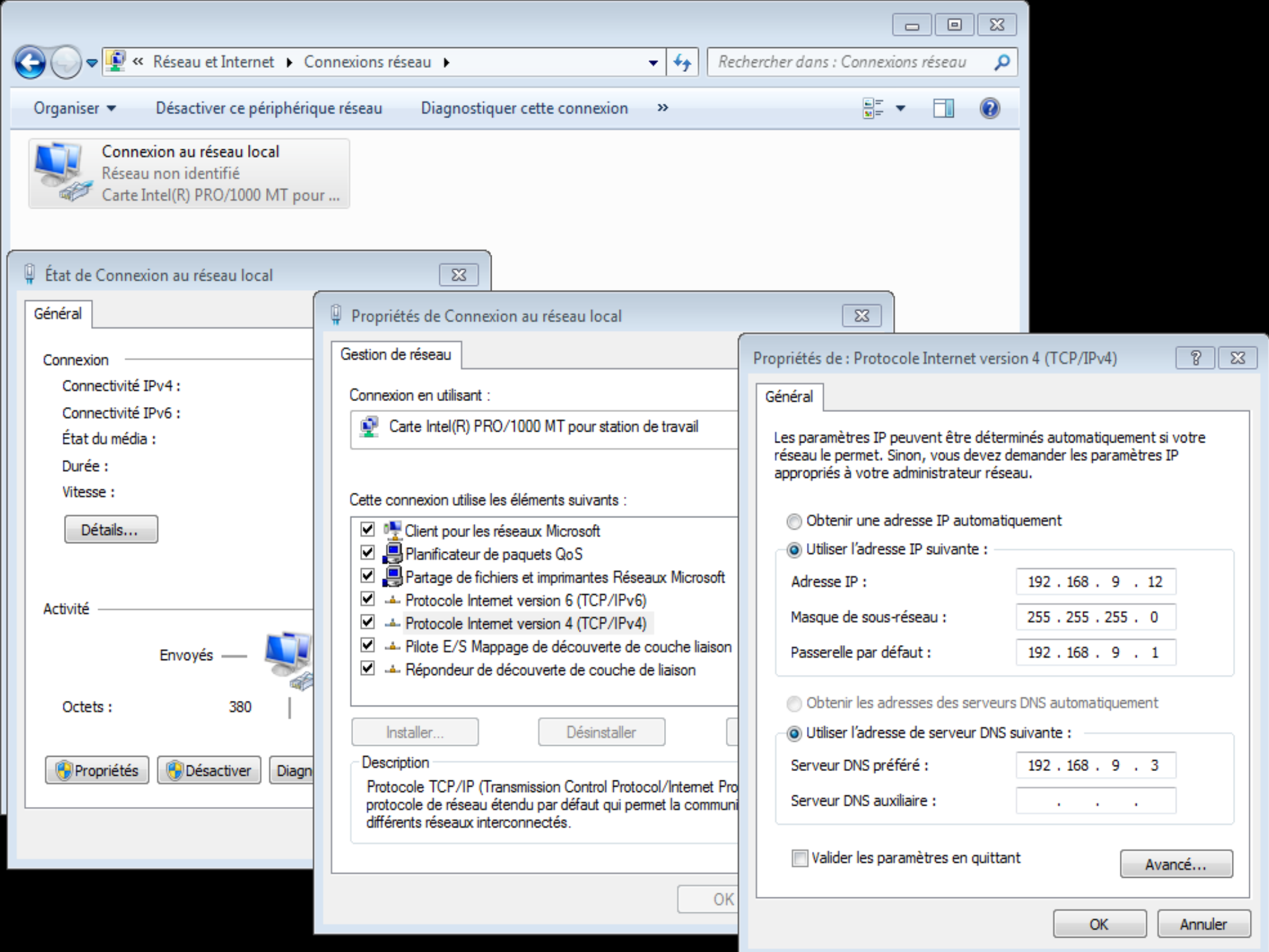
- mount -t cifs //adresse_serveur/partage point_montage -o user=utilisateur

- Ou

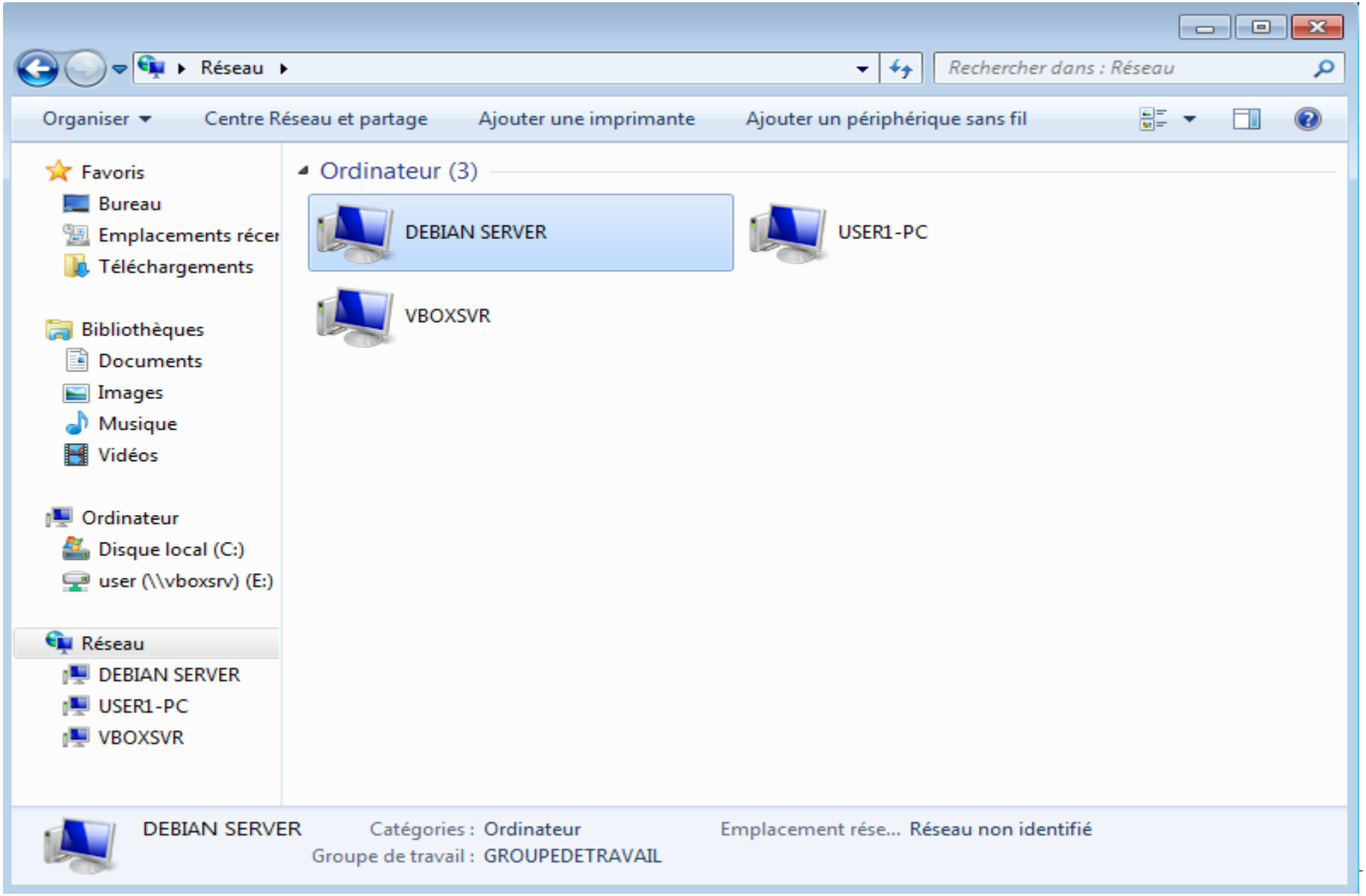
- /etc/fstab
  - //adresse_serveur/partage point_montage cifs user=utilisateur

Côté client
Credentials

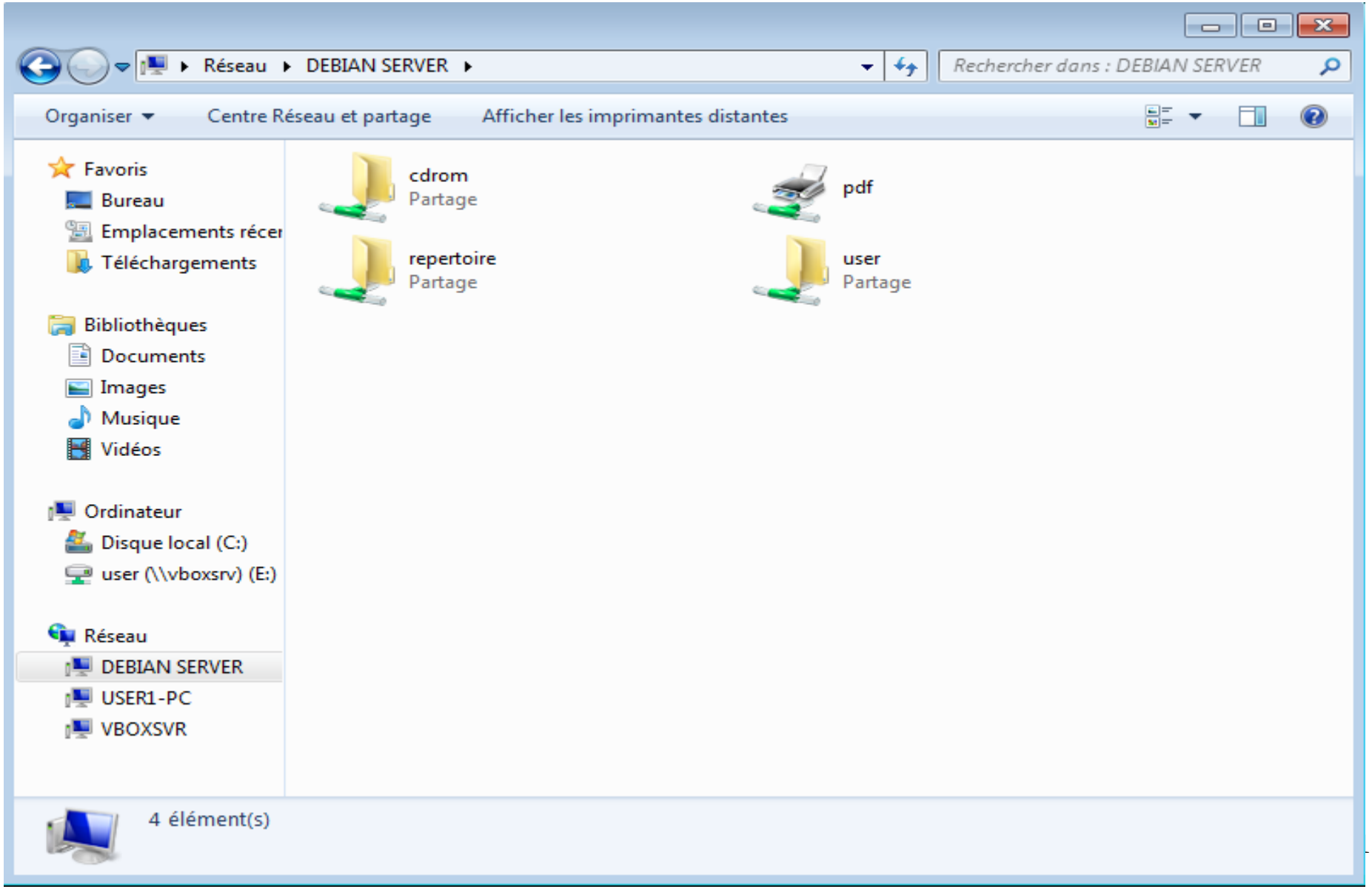
- /home/user/.fichier :
  - username=user
  - password=motdepasse
- mount -t cifs //adresse_serveur/partage point_montage -o credentials=/home/user/.fichier
- /etc/fstab
  - //adresse_serveur/partage point_montage cifs credentials=/home/user/.fichier


« Réseau et Internet ▸ Connexions réseau ▸
Rechercher dans : Connexions réseau
Organiser
Désactiver ce périphérique réseau
Diagnostiquer cette connexion
»
Connexion au réseau local
Réseau non identifié
Carte Intel(R) PRO/1000 MT pour ...
État de Connexion au réseau local
Général
Connexion
Connectivité IPv4 :
Connectivité IPv6 :
État du média :
Durée :
Vitesse :
Détails...
Activité
Envoyés
Octets :
380
Propriétés
Désactiver
Diagn
Propriétés de Connexion au réseau local
Gestion de réseau
Connexion en utilisant :
Carte Intel(R) PRO/1000 MT pour station de travail
Cette connexion utilise les éléments suivants :
Client pour les réseaux Microsoft
Planificateur de paquets QoS
Partage de fichiers et imprimantes Réseaux Microsoft
Protocole Internet version 6 (TCP/IPv6)
Protocole Internet version 4 (TCP/IPv4)
Pilote E/S Mappage de découverte de couche liaison
Répondeur de découverte de couche de liaison
Installer...
Désinstaller
Description
Protocole TCP/IP (Transmission Control Protocol/Internet Pro
protocole de réseau étendu par défaut qui permet la communi
différents réseaux interconnectés.
OK
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 9 . 12
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 9 . 1
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192 . 168 . 9 . 3
Serveur DNS auxiliaire : . . .
Valider les paramètres en quittant
Avancé...
OK
Annuler

Vérification du partage



Vérification du partage



Plan de la 4ème partie

- Serveur Web
- Messagerie électronique
- Connexion à distance par SSH
- Pare-Feu

Serveur Apache

- Caractéristiques :
  - Popularité
  - Stabilité
  - Structure modulaire

Installation

- Côté serveur :
  - apt-get install apache2
- Côté client :
  - apt-get install iceweasel

    ou
  - apt-get install lynx

Configuration (côté serveur)

- Configurations générales
  - /etc/apache2/apache2.conf
- Configurations spécifiques pour chaque site web
  - /etc/apache2/sites-available/*
- Configurations spécifiques pour chaque module
  - /etc/apache2/mods-available/*

Configuration (côté serveur)
Exemple

- ServerRoot /etc/apache2
- ErrorLog /var/log/apache2/error.log
- Listen 80
- DocumentRoot /var/www
- <Directory /var/www>

  allow from all

  </Directory>

Site web par défaut

- /etc/apache2/sites-available/default
- <VirtualHost *:80>

```
        ServerAdmin  root@localhost
        DocumentRoot  /var/www
        <Directory  /var/www>
                allow  from  allow
        </Directory>
        ...
</VirtualHost>
```

Plusieurs sites/une seule adresse IP

Hôtes vituels

- /etc/apache2/sites-available/site1
- <VirtualHost *:80>

  ServerName nom.domaine

  DocumentRoot /var/www/site1

  </VirtualHost>
- a2ensite site1

Sites web personnels

- Chargement du module « userdir »
  - a2enmod userdir
- Création du répertoire « public_html » sous /home/$USER
  - Peut modifié dans /etc/apache2/mods-available/userdir.conf
- Consultation à l'aide de l'adresse serveur.domaine/~$USER

Serveur de messagerie

- MTA (MAil Transfer Agent) : Agent de Transfert de Mails
  - Envoi et réception de messages électroniques
- MDA (Mail Delivery Agent) : Agent de délivrance de Mails
  - Remise des messages
- MUA (Mail User Agent) : Client de messagerie

Protocole SMTP

- SMTP (Simple Mail Transfer Protocol)
  - Protocole utilisé par un MTA
  - Pour le transfert de messages électroniques vers les serveurs de messagerie.

Postfix

- Postfix
  - C'est un MTA open-source
  - utilisé par de nombreux hébergeurs et fournisseurs d'accès.
  - Se caractérise par sa simplicité de configuration

Postfix
Comptes de messagerie

- Comptes unix créés sur le serveur
  - user@domaine
- Alias
  - /etc/alias

    webmaster : root

    hostmaster : root
- Génération de la base à partir de /etc/alias
  - postalias /etc/alias

Postfix
Configuration

- /etc/postfix/main.cf
  - myorigin = domaine vu de l'extérieur
  - mydestination = domaine à destination
  - mynetwork = réseau/masque
  - home_mailbox = Maildir/

Postfix
Domaines virtuels

- /etc/postfix/main.cf
  - virtual_alias_domain domaine1, domaine2
- Affectation des boîtes aux lettres aux différents comptes :
  - virtual_alias_maps=hash:/etc/postfix/virtual
- /etc/postfix/virtual
  - adresse_mail compte_unix
- postmap /etc/postfix/virtual

IMAP4

- IMAP4
  - L'un des protocoles utilisés par les MDA
  - Télécharge les en-têtes des messages et donne au client le choix de consulter, effacer, déplacer, etc.

Courier-IMAP

- Courier-IMAP
  - Suite logicielle fournissant un ensemble de services de gestion de courriers électroniques.

Courier-IMAP

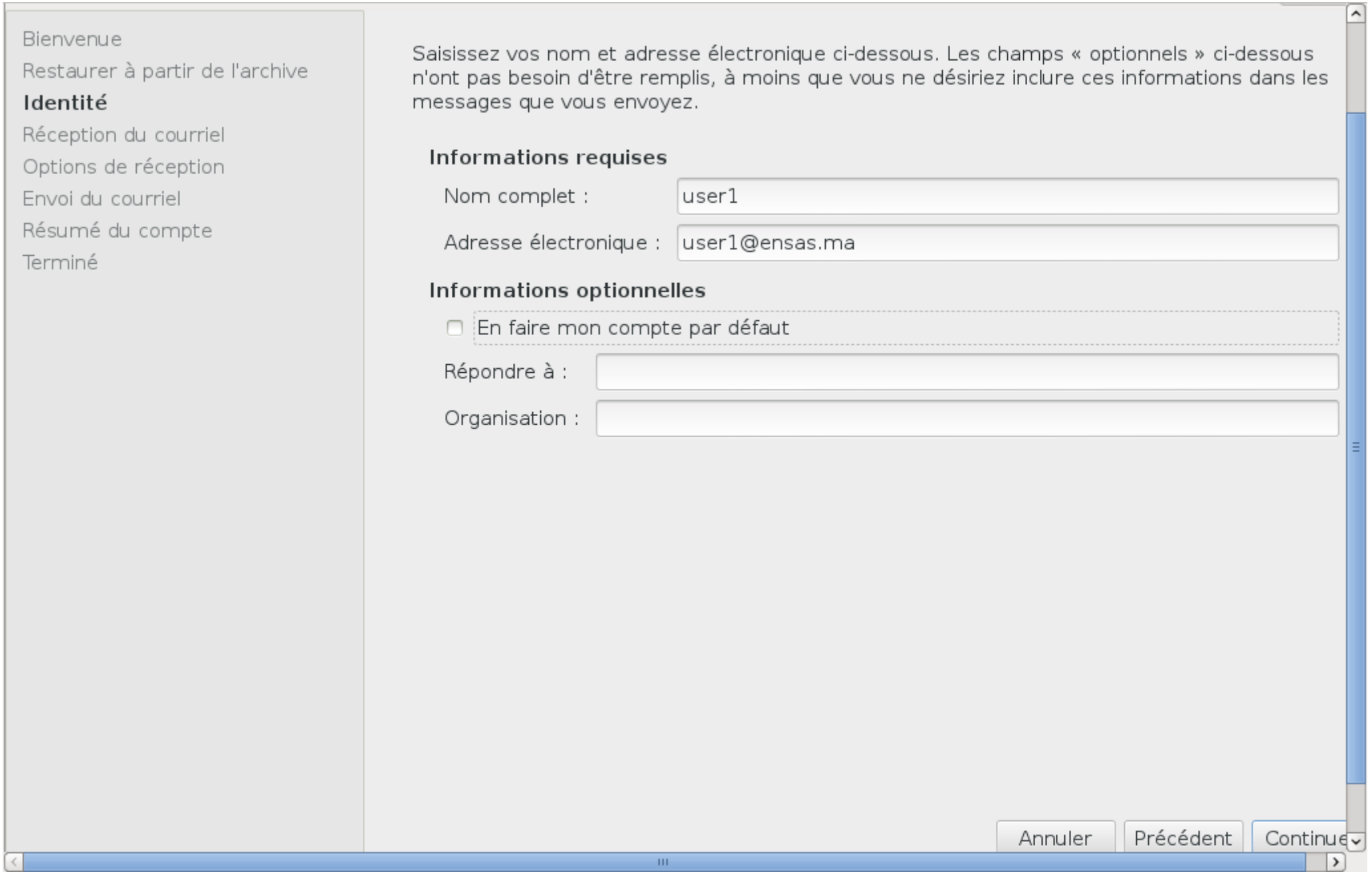
- Configuration
  - /etc/courier/imapd

    MAILDIRPATH = Maildir

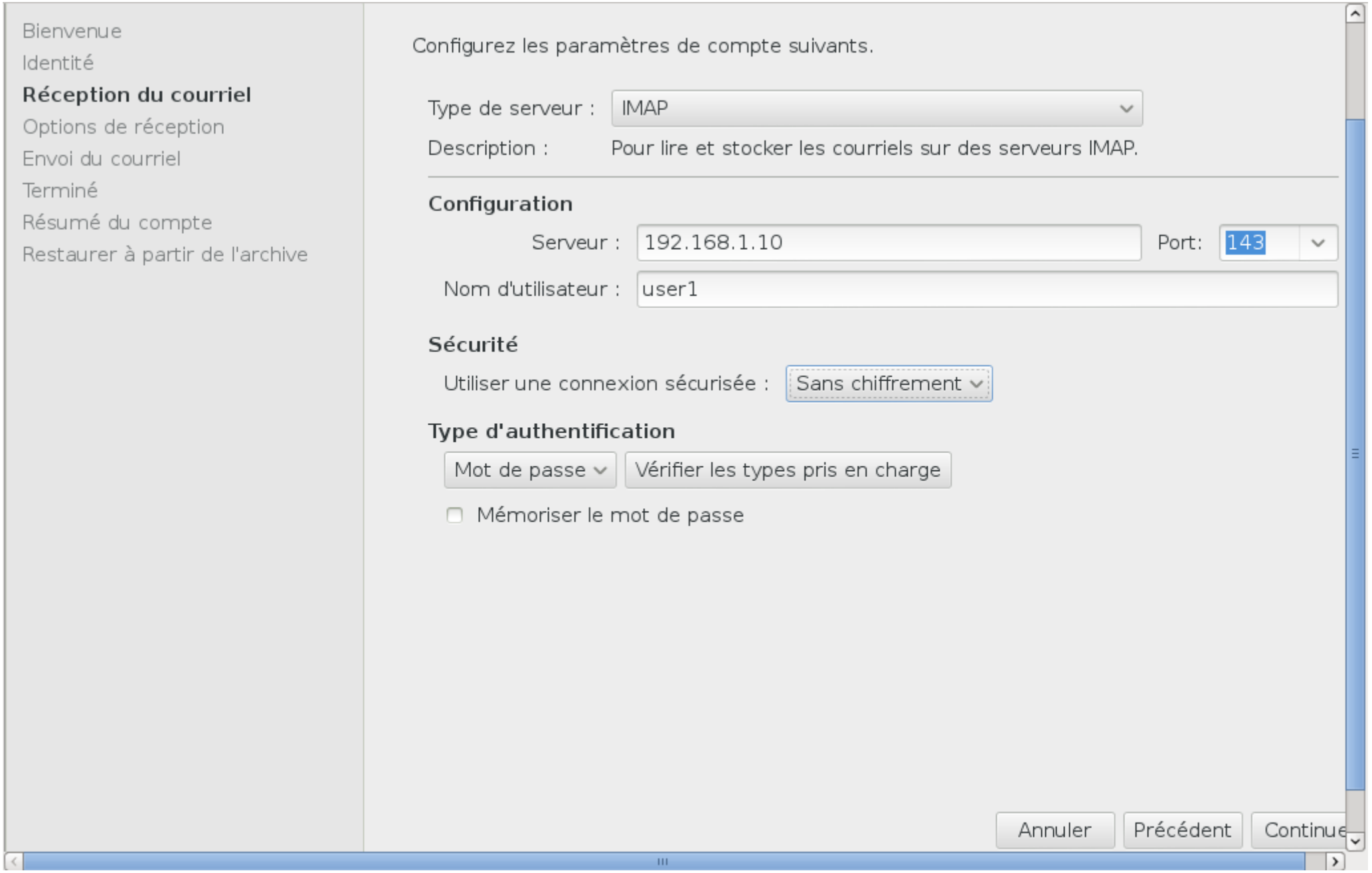
Installation

- Côté serveur :
  - apt-get install postfix
  - apt-get install courier-imap
- Côté client
  - apt-get install evolution

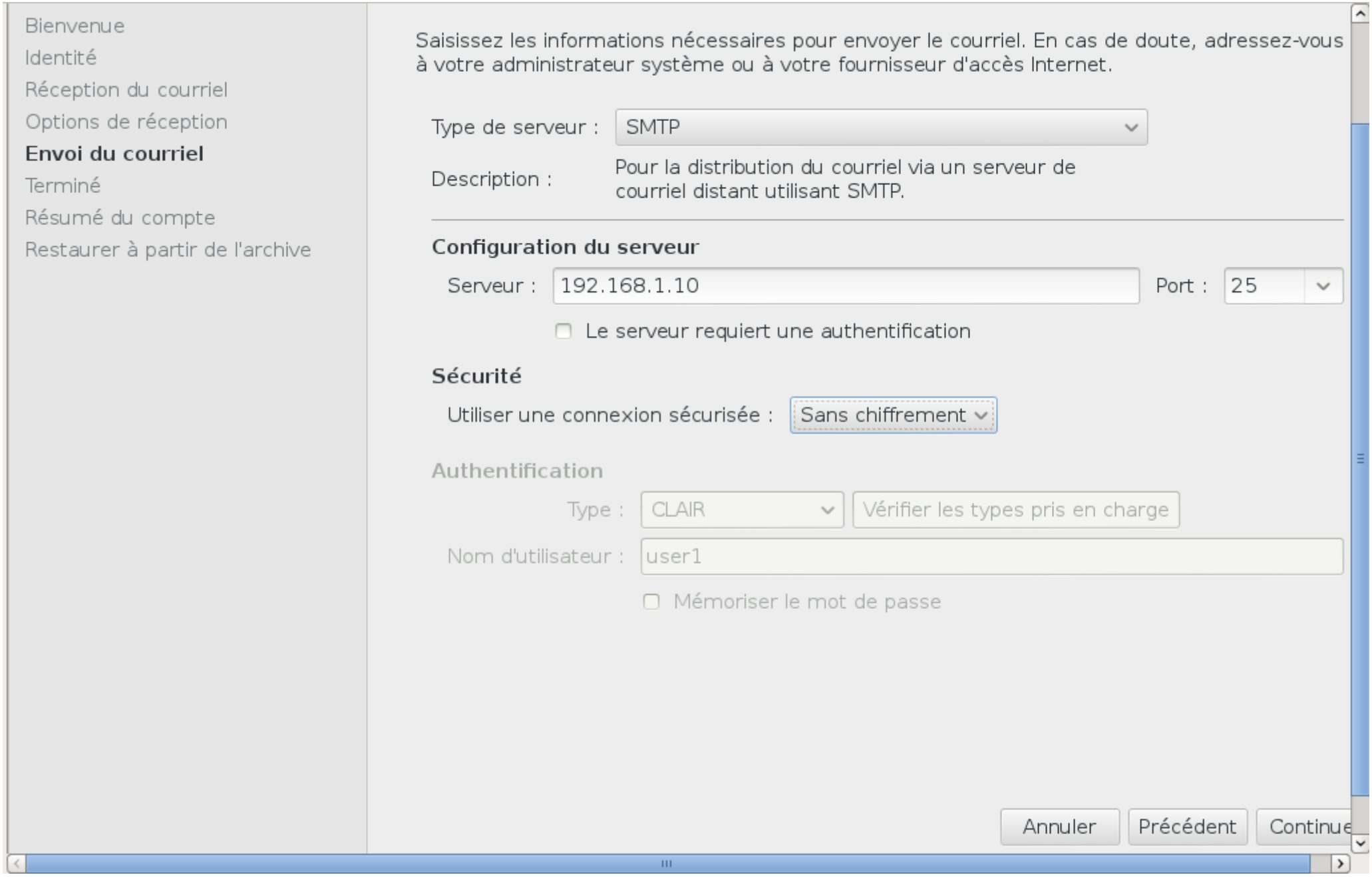
Client de messagerie



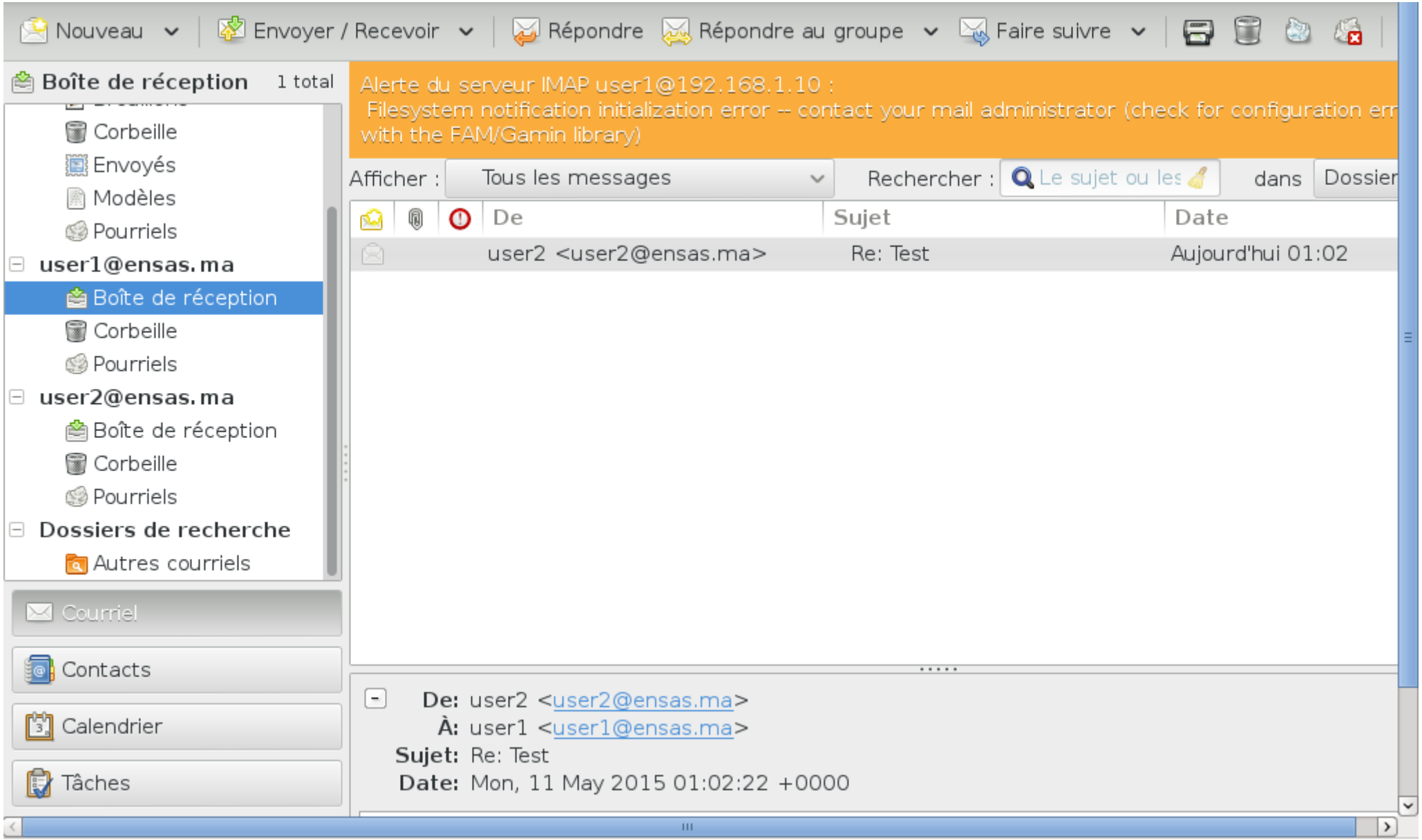
Client de messagerie



Client de messagerie



Client de messagerie



Connexion à distance par SSH

- SSH :
  - Protocole de connexion à distance à l'aide d'un compte unix local au serveur
  - Apporte des services d'authentification et de confidentialité
  - Considéré comme « telnet sécurisé »

Installation

- Côté serveur :
  - apt-get install openssh-server
- Côté client :
  - apt-get install openssh-client

Authentification par mot de passe

- ssh user@serveur
  - Vérification de la clé ECDSA affichée avec celle stockée sur le serveur
  - ssh-keygen -l (côté serveur)
- Une fois c'est vérifié, la clé est stockée cryptée dans ~/.ssh/known_hosts

Authentification par mot de passe

- ssh user@serveur
  - Vérification de la clé ECDSA affichée avec celle stockée sur le serveur
  - ssh-keygen -l (côté serveur)
- Une fois c'est vérifié :
  - la clé est stockée cryptée dans ~/.ssh/known_hosts
  - Le mot de passe de user est demandé

Authentification par clés

- Utilisation de clés stockées sur le client
- Création d'une clé publique et une clé privée (côté client) :
  - ssh-keygen -t rsa
  - .ssh/id_rsa et .ssh/id_rsa.pub
- Copie de la clé publique dans .ssh/authorized_keys du serveur

Copie de fichiers par SCP

- Copie à l'aide du protocole SSH.
- Copie d'un fichier local vers le serveur :
  - scp user@server : /fichier_distant fichier_local
- Téléchargement d'un fichier distant :
  - scp fichier_local user@server : /fichier_distant

Tunnels SSH

- Utilisation de SSH pour sécuriser une communication client-serveur basée sur un protocole peu sécurisé
  - ssh -L port : cible_trafic : port_cible user@serveur

Pare-Feu

- Gestion de filtrage de paquets IP
- Peut fonctionner selon deux modes :
  - Tout ce qui n'est pas autorisé est interdit
  - Tout ce qui n'est pas interdit est autorisé
- Utilise l'outils « iptables »
- Iptables filtre le trafic en transit dans un routeur, le trafic entrant et le trafic sortant.

Politique par défaut

- Affichage de la politique par défaut :
  - iptables -S
- Modification de la politique par défaut :
  - iptables -P chaine action

    Chaine = INPUT, OUTPUT ou FORWARD

    Action = ACCEPT ou DROP

Ajout de régles iptables

- iptables -A chaine -s ip_source -d ip_destination -p protocole --dport port -j action
- Exemple :
  - iptables -A FORWARD -s 192.168.9.0/24 -d 192.168.8.9/32 -p icmp -j DROP

Gestion des règles

- Suppression de toutes les règles
  - iptables -F
- Affichage des numéros des règles :
  - iptables -L chaine --line-numbers -n
- Suppression d'une règle :
  - iptables -D chaine numéro
- Insertion d'une règle :
  - iptables -I chaine numéro condition action

Gestion des flux retours

- Autoriser les flux retours qui sont des réponses à un flux en sortie explicitement autorisé.
  - iptables -A chaine -m state --state ESTABLISHED,RELATED -j ACCEPT
- ESTABLISHED : paquets en réponse à un flux aller autorisé
- RELATED : paquets issus d'une nouvelle connexion établie à l'initiative d'une connexion autorisée.